(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 43 21 849 A1**

(51) Int. Cl.[6]: G 07 C 9/00

(21) Aktenzeichen: P 43 21 849.0
(22) Anmeldetag: 1. 7. 93
(43) Offenlegungstag: 12. 1. 95

DE 43 21 849 A1

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Mönig, A., Dipl.-Ing., Pat.-Ass., 7030 Böblingen

(72) Erfinder:
Klepser, Günter, 72119 Ammerbuch, DE; Schaal, Albert, 72076 Tübingen, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Rücksetzung einer gesperrten PIN oder eines gesperrten Kennworts

(57) Die Erfindung sieht eine/ein erweiterte(s) PIN/Kennwort vor, die wesentlich mehr Stellen umfaßt, als die/das einfache mit beispielsweise vier Stellen. Diese(s) erweiterte PIN/Kennwort wird dazu benutzt, um die/das durch zu viele Fehlversuche oder Verlust gesperrte PIN/Kennwort wieder zu entsperren und benutzbar zu machen. Dem einzelnen Benutzer selbst ist es durch die Kenntnis der/des erweiterten PIN/Kenntworts möglich, ohne in Anspruchnahme einer besonders autorisierten Person oder Institution die Funktion seiner/seines üblichen PIN/Kennworts wieder herzustellen und damit Zugriff zu geschützten Daten und Geräten zu haben.

DE 43 21 849 A1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Aufheben der Sperrung des Zugriffs zu Geräten, Daten und sonstigen Vorrichtungen, zu denen durch Eingabe einer persönlichen Identifikationsnummer, der sogenannten PIN bzw. eines Kennworts Zugriff erreichbar ist, gemäß dem Oberbegriff des Anspruchs 1.

Viele Geräte, die geschützte Daten oder Funktionen enthalten, oder auch besondere Wertgegenstände, sind für die Benutzer über die persönliche Identifikationsnummer, die sogenannte PIN oder ein Kennwort zu öffnen und können dann benutzt werden. Als Beispiel für solche Geräte sei hier nur auf Geldausgabegeräte bei Banken, oder auf geschützte Dateien in Computernetzwerken oder sonstige schützenswerte Vorrichtungen hingewiesen. Das Anwendungsspektrum ist weit gefächert.

In der Regel hat eine PIN so wenige Stellen, üblich sind vier, daß man sie sich auswendig merken kann. Dies gilt sinngemäß auch für ein Kennwort. Die PIN besteht überlicherweise tatsächlich aus einzelnen Ziffern, während ein Kennwort aus Buchstaben oder aus einer Kombination von Buchstaben und Ziffern bestehen kann.

Es kommt nun in der Praxis immer wieder vor, daß die PIN bzw. das Kennwort falsch eingegeben wird, entweder weil man es nicht richtig behalten hat oder weil man sich bei der Eingabe vertippt. Um den Inhalt des Gerätes oder die Integrität der Daten zu schützen, werden nur wenige Fehlversuche, beispielsweise drei, zugelassen. Hat der Fehlerzähler einen vorgegebenen Wert erreicht, dann wird das Gerät bzw. die Datei gesperrt, so daß man selbst bei Anwendung der korrekten PIN bzw. des richtigen Kennworts keinen Zugriff mehr hat. Die PIN bzw. das Kennwort ist dann als gesperrt anzusehen. Es gibt jedoch auch Fälle, bei denen ein rechtzeitiger erfolgreicher Versuch den Fehlerzähler wieder zurückstellt und damit die Möglichkeit gegeben ist, den Zählerstand wieder bis zur vorgebenen Höchstmarke aufzufüllen.

Ist der Zugang zu einem Gerät, einer Datei oder einem Vorgang gesperrt, dadurch daß die PIN selbst oder das Kennwort wegen Überschreitung der Fehlversuche gesperrt ist, ist es höchst mühsam, wieder Zugriff zu erhalten. Der Benutzer selbst kann das gesperrte Gerät nicht entsperren bzw. die PIN oder das Kennwort wieder aktivieren. Es muß für diesen Vorgang eine besondere priviligierte Person die Entsperrung vornehmen. In der Praxis ist dies oft höchst mühsam und aufwendig.

Es ist Aufgabe vorliegender Erfindung, ein Verfahren anzugeben, mit dem der einzelne Benutzer selbst die Sperrung des Gerätes aufheben kann bzw. die Funktion der PIN bzw. des Kennworts selbst wieder regenerieren kann. Dazu soll es nicht nötig sein, eine besondere priviligierte Person in Anspruch nehmen zu müssen.

Diese Aufgabe wird erfindungsgemäß bei dem Verfahren gemäß dem Oberbegriff des Anspruchs 1 dadurch gelöst, daß eine erweiterte PIN/erweitertes Kennwort vorgesehen ist, die erweiterte PIN/das erweiterte Kennwort jedem einzelnen Benutzer, vorzugsweise zusammen mit der/dem normalen einfachen PIN/Kennwort bekanntgegeben wird, zur Aufhebung der Sperrung die/das erweiterte PIN/Kennwort eingegeben wird und daß diese Eingabe der/des erweiterten PIN/Kennworts durch den einzelnen Benutzer selbst erfolgt.

Vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens sind in den Unteransprüchen niedergelegt. Die sich dabei ergebenden Vorteile liegen auf der Hand oder werden nachfolgend in der speziellen Beschreibung näher erläutert.

Gemäß der Erfindung wird dem ausgesperrten Benutzer die Möglichkeit gegeben, das Gerät selbst durch eine erweiterte PIN bzw. durch ein erweitertes Kennwort zu entsperren. Anders ausgedrückt, die Funktion der normalen PIN wird durch den Benutzer selbst durch Eingabe der erweiterten PIN wiederhergestellt. Im folgenden wird der Ausdruck PIN auch für den Ausdruck Kenntwort benutzt werden, um die Darstellung einfacher zu halten. Die Erfindung bewirkt damit den erheblichen Vorteil, einer wesentlich einfacheren Prozedur der Entsperrung der PIN bzw. des Kennworts.

Die erfindungsgemäß vorgesehene erweiterte PIN ist in vorteilhafter Weise mit deutlich mehr Stellen ausgestattet. Der Benutzer kann sie sich deshalb normalerweise nicht auswendig merken. Es ist aus verschiedenen Gründen besonders zweckmäßig, die erweiterte PIN erst dann benutzbar zu machen, wenn das Gerät gesperrt ist, beispielsweise nach Erreichen der vorgegebenen Anzahl von Fehlversuchen mit der einfachen PIN. Dem einzelnen Benutzer werden beide PINs zusammen bekannt gegeben, er selbst muß dafür sorgen, daß sie gesichert aufbewahrt werden. Dies gilt insbesondere für die erweiterte PIN, die ja nur im Extremfall benutzt wird, wenn die einfache PIN nicht mehr benutzbar ist, entweder weil sie verlorengegangen ist oder weil die vorgegebene Anzahl von Fehlversuchen erreicht wurde.

Nach einer zweckmäßigen Gestaltung der erweiterten PIN steht diese zur einfachen PIN in einem bestimmten Bezug. Beispielsweise können die letzten vier Stellen der erweiterten PIN/der vierstelligen einfachen PIN gleichen.

Nach einer zweckmäßigen Ausführungsform gemäß der Erfindung, die den Schutz der Funktionen und Daten auch nach mehrmaligem Regenieren erhält, ist vorgesehen, daß nach einer gewissen Anzahl von Fehlversuchen mit der erweiterten PIN, in einen neuen, den erweiterten Sperrstatus, gegangen wird. Auch dann ist eben das Gerät bzw. die Funktion nicht nutzbar. Aus diesem erweiterten Sperrstatus, der im allgemeinen sehr selten vorkommen dürfte, kann man dann allerdings wieder nur mit Hilfe eines priviligierten Benutzers herauskommen, der autorisiert ist, diesen Zustand aufzuheben.

Eine einfache mathematische Sicherheitsanalyse ergibt, daß durch die erweiterte PIN, welche deutlich mehr Stellen als die einfache PIN aufweist, die Sicherheit in beiden Fällen etwa die gleiche ist. Dies wird nachfolgend erläutert.

Bei einer n-stelligen PIN im Dezimalsystem und c erlaubten Fehlversuchen sowie einer m-stelligen erweiterten PIN mit d weiteren erlaubten Fehlversuchen ist die Wahrscheinlichkeit des zufälligen Öffnens bis zum Sperren

$$w1 = c/(10^n).$$

Das Regenerieren mit der m-stelligen erweiterten PIN und ebenfalls drei erlaubten Fehlversuchen eröffnet folgende neue Möglichkeit des zufälligen Öffnens:

$$w2 = d/(10^m).$$

Die Gesamtwahrscheinlichkeit des zufälligen Öffnens beträgt nun

$w_{ges} = w1 + w2$

Da die erweiterte PIN deutlich mehr Stellen hat als die einfache, ergibt sich:

$w_{ges} \sim w1$.

Die Vorteile der Erfindung sind generell darin zu sehen, daß der einzelne Benutzer bzw. die einzelne Benutzerin die Möglichkeit hat, das gesperrte Gerät selbst wieder zu entsperren. Obwohl diese Möglichkeit gegeben wird, verringert sich die Sicherheit gegen unbefugtes Benutzen praktisch nicht, wie die vorstehende mathematische Analyse zeigt. Auf der anderen Seite wird der organisatorische Aufwand, der durch ein aufwendiges Entsperren des Sicherheits-sensitiven Gerätes durch einen priviligierten Systemadministrator nötig wäre, erheblich seltener und geringer, da der Systemadministrator nur noch in Fällen der gesperrten erweiterten PIN von Nöten ist.

Bei Massenanwendungen von Geräten, wie z. B. Chipkarten, und Entsperrung einzelner Bereiche auf dieser Chipkarte durch Eingabe von PIN, ist die durch die vorliegende Erfindung eingeführte Regenierungsmöglichkeit für gesperrte Karten von besonderer Wichtigkeit.

Ein Beispiel für eine derartige Massenanwendung kann eine medizinische Chipkarte für Diabetiker sein, die mit einer vierstelligen PIN geschützt ist. Der Patient bzw. die Patientin hat diese PIN mit einem sogenannten PIN-Brief erhalten, also in einem geschlossenen Umschlag, wie es auch bei den PIN für die Euro-Scheckkarten üblich ist. In diesem Umschlag befindet sich auch die erweiterte PIN, beispielsweise mit zehn Stellen. Dieser PIN-Brief wird an einem sicheren Ort aufbewahrt und der Patient bzw. die Patientin lernt die vierstellige PIN auswendig. Mit dieser vierstelligen PIN ist dem Patienten der Zugriff zu der Chipkarte erlaubt.

Gesetzt den Fall, der Patient ist zerstreut oder er vertut sich aus anderen Gründen beim Eingeben, so sperrt sich die Karte beispielsweise nach fünf Fehlversuchen. Um Mißbrauch zu verhindern, müßte nun der Patient zu einer dazu autorisierten Instanz gehen, um sich die Karte wieder entsperren zu lassen. Diese Instanz, beispielsweise eine Krankenkasse, hat die Autorität, die Karten zu entsperren. Dazu muß die Identität des Karteninhabers sorgfältig geprüft werden. Andererseits kann die Instanz, die Krankenkasse, aber keine medizinischen Daten lesen, die auf der Karte enthalten sind. Damit wird sichergestellt, daß es sich einerseits um den rechtmäßigen Eigentümer der zu entsperrenden Karte handelt und daß andererseits der Datenschutz nicht verletzt wird.

Vorliegende Erfindung eröffnet die Möglichkeit, die Karte zu regenerieren, ohne daß die autorisierte Instanz, wie im vorliegenden Beispielsfall die Krankenkasse, aufsuchen zu müssen. Entweder hat der Patient selbst einen Personal Computer mit Chipkartenleser zu Hause, wobei er als Diabetiker zu Hause seine Selbstüberwachungsdaten auf die Chipkarte eingibt, oder er geht zum Hausarzt und regeneriert mit der inzwischen herausgesuchten erweiterten PIN selbst seine Karte.

Erst, wenn auch bei der Anwendung der Entsperrung mit Hilfe der erweiterten PIN eine gewisse Anzahl von Versuchen fehlgeschlagen ist, wird die Karte endgültig gesperrt und kann offiziell nur bei der autorisierten Instanz entsperrt werden.

Die Frage der Sicherheit bzw. der Vergrößerung der Unsicherheit läßt sich an folgendem Beispiel darlegen: Angenommen der erste Zähler, der für die normale, einfache, beispielsweise vierstellige PIN zuständig ist, sperrt bei fünf Versuchen und der zweite Zähler, der die Regenerierungsvorgänge registriert, welche mittels der erweiterten PIN vorgenommen werden, sperrt bei acht Versuchen, dann ergibt sich folgende Rechnung:

$w1 = 5 : 10\,000$, also $w1 = 0{,}0005$

$w2 = 8 : 10\,000\,000\,000$, also $w2 = 0{,}000\,000\,0008$.

Die Gesamtwahrscheinlichkeit des zufälligen Öffnens oder Zugang beträgt nun

$w_{ges} = w1 + w2$

und damit

$w_{ges} \sim 0{,}0005$.

Wie dieses Beispiel zeigt, ist der Zuwachs an Unsicherheit durch die erweiterte PIN vernachlässigbar klein.

Patentansprüche

1. Verfahren zum Aufheben der Sperrung des Zugriffs zu Geräten, Daten und sonstigen Vorrichtungen, zu denen durch Eingabe einer persönlichen Identifikationsnummer, der sogenannten PIN, bzw. eines Kennworts Zugriff erreichbar ist, wobei der Zugriff nach Eingabe einer gewissen, vorbestimmten Anzahl von Fehlversuchen gesperrt wird oder der Zugriff bei Verlust der PIN nicht möglich ist, gekennzeichnet durch folgende Schritte:
   a) Vorsehen einer/eines erweiterten PIN/Kennworts;
   b) Bekanntgabe der/des erweiterten PIN/Kennworts an jeden einzelnen Benutzer, vorzugsweise zusammen mit der/dem normalen, einfachen PIN/Kennwort;
   c) Eingabe der/des erweiterten PIN/Kennworts zur Aufhebung der Sperrung, und
   d) Eingabe der/des erweiterten PIN/Kennworts durch den einzelnen Benutzer selbst.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die/das erweiterte PIN/Kennwort wesentlich mehr, vorzugsweise zehn Stellen enthält als die/das normale, einfache PIN/Kennwort, die/das üblicherweise vier Stellen enthält.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die/das erweiterte PIN/Kennwort mit der/dem normalen, einfachen PIN/Kennwort in bestimmtem Bezug steht, insbesondere die letzten vier Stellen einer/eines erweiterten PIN/Kennworts der/des vierstelligen normalen, einfachen PIN/Kennworts gleichen.
4. Verfahren nach einem der vorigen Ansprüche, dadurch gekennzeichnet, daß die Anzahl der möglichen Versuche, die Sperrung des Zugriffs mittels der/des erweiterten PIN/Kennworts aufzuheben, begrenzt ist, insbesondere auf fünf Fehlversuche, und daß nach Erreichen dieser Anzahl in einen erweiterten Sperrstatus gegangen wird.
5. Verfahren nach einem der vorigen Ansprüche, dadurch gekennzeichnet, daß die/das erweiterte PIN/Kennwort erst dann benutztbar und wirksam

ist, wenn der Zugriff über die/das einfache PIN/ Kennwort gesperrt ist.